CLAIMS

1. A method of operating a trusted computing system, the method comprising an assessor receiving a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report.

2. A method according to claim 1, wherein the assessor updates the trust policies of multiple computing devices in accordance with the report.

3. A method according to claim 1, wherein the assessor updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

4. A method according to claim 1, wherein the assessor updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

5. A method according to claim 1, wherein the assessor requests the first computing device to make the report.

6. A method according to claim 1, wherein the first computing device is caused to report by being started-up or reset, or by an undesirable event occurring.

7. A method according to claim 1, wherein the first computing device is caused to report periodically.

8. A method according to claim 1 in which the second computing device authenticates the trust policy update issued by the assessor before accepting it.

9. A method of operating a trusted computing system in which a first computing device has a trusted component which issues a report pertaining to the trustworthiness of the first computing device wherein a trust policy controller receives said report from the

trusted component and updates the trust policy of a second computing device in accordance with said report.

10. A method of operating a trusted computing system comprising multiple computing devices wherein a trust policy controller determines the trust policy for each of said computing devices in accordance with the trustworthiness of other of said multiple computing devices as determined from reports received by the controller pertaining to the trustworthiness of each computing device.

11. An assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device.

12. An assessor according to claim 11, wherein the updater is arranged to update the trust policies of multiple computing devices in accordance with the report and the transmitter is arranged to transmit the updated policies to the multiple computing devices.

13. An assessor according to claim 11, wherein the updater updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

14. An assessor according to claim 11, wherein the updater updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

15. An assessor according to claim 11 further comprising a requestor, for requesting the report from the first computing device.

16. A system comprising an assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device, and the system further comprising first and second computing devices, wherein at least the first computing device comprises a reporter for sending a trustworthiness report to the assessor and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter.

17. A system as claimed in claim 16 in which the reporter comprises a trusted component associated with the first computing device.

18. A system comprising multiple computing devices and a trust policy controller which serves to determine the trust policy of said computing devices; each of said computing devices having associated with it a trust policy memory to store a trust policy for that computing device, and a trusted component which issues a report pertaining to the trustworthiness of that computing device; wherein the controller receives reports from the trust components and updates the trust policy in the trust policy memory of each computing device in accordance with the trustworthiness of other of said multiple computing devices as determined from said reports.